Configuring Secure Domain Routers on Cisco IOS XR Software

Secure domain routers (SDRs) are a means of dividing a single physical system into multiple logically separated routers. SDRs are isolated from each other in terms of their resources, performance, and availability.

Note SDRs were previously known as Logical Routers (LRs). The name was changed for Release 3.3.0.

Feature History for Configuring Secure Domain Routers on Cisco IOS XR Software

Release	Modification
Release 3.2	This feature was supported on Cisco XR 12000 Series Routers.
Release 3.3.0	This feature was supported on the Cisco CRS-1. The term Logical Router (LR) was changed to Secure Domain Router (SDR). Support was added for distributed route processor cards (DRPs) and DRP pairs on the Cisco CRS-1. Support was added for SDR-specific software package activation on the Cisco CRS-1 and Cisco XR 12000 Series Routers.
Release 3.4.0	No modification.

Contents

Prerequisites for Configuring Secure Domain Routers

Before configuring SDRs, the following conditions must be met:

Initial configuration

- The router must be running the Cisco IOS XR software, including a Designated System Controller (DSC).
- The root-system username and password must be assigned as part of the initial configuration.
- For more information on booting a router and performing initial configuration, refer to *Cisco IOS XR Getting Started Guide*.

Required cards for each SDR

- In Cisco CRS-1 routers, an additional RP pair, DRP or DRP pair must be installed in each line card (LC) chassis to manage each SDR in the system.
- In Cisco XR 12000 Series Routers, an additional RP or RP pair must be installed to manage each SDR in the system.
- For additional information on DRPs, refer to *Cisco CRS-1 Carrier Routing System 16-Slot Line Card Chassis System Description*. For instructions on installing DRPs, refer to *Installing the Cisco CRS-1 Carrier Routing System 16-Slot Line Card Chassis*.

Task ID requirements

- You must be in a user group associated with a task group that includes the proper task IDs for SDR commands.
- For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Software Version Requirements for the Cisco XR 12000 Series Router

- Multiple SDRs, including non-owner SDRs, are supported on Cisco XR 12000 Series Router running Cisco IOS XR Software Release 3.2 or higher.

Software Version Requirements for the Cisco CRS-1

- Cisco IOS XR Software Releases 2.0, 3.0, and 3.2 support only one owner SDR on the Cisco CRS-1. Multiple (non-owner) SDRs are not supported in these releases. The owner SDR cannot be added or removed from the configuration.
- Multiple SDRs, including non-owner SDRs, are supported on Cisco CRS-1 running Cisco IOS XR Software Release 3.3.0 or higher.

Maximum SDR configurations

- The Cisco CRS-1 supports a maximum of eight SDRs, including one owner SDR and up to seven non-owner SDRs.
- For the Cisco XR 12000 Series Router, we recommend a maximum of four SDRs, including one owner SDR and up to three non-owner SDRs.

Information About Configuring Secure Domain Routers

Review the following topics before configuring secure domain routers:

What Is a Secure Domain Router?

Cisco routers running Cisco IOS XR software can be partitioned into multiple, independent routers known as *secure domain routers* (SDRs). SDRs are a means of dividing a single physical system into multiple logically separated routers. SDRs perform routing functions the same as a physical router, but they share resources with the rest of the system. For example, the software, configurations, protocols, and routing tables assigned to an SDR belong to that SDR only, but other functions, such as chassis-control and switch fabric, are shared with the rest of the system.

Owner SDR and Administration Configuration Mode

The *owner SDR* is created at system startup and cannot be removed. This owner SDR performs system-wide functions, including the creation of additional *non-owner* SDRs. You cannot create the owner SDR because it always exists, nor can you completely remove the owner SDR, because it is necessary to manage the router. By default, all nodes in the system belong to the owner SDR.

The owner SDR also provides access to the Administration EXEC and Administration configuration modes. Only users with root-system privileges can access the Administration modes by logging in to the primary Route Processor for the owner SDR (called the Designated Shelf Controller, or DSC).

Administration modes are used for the following purposes:

- Create and remove additional non-owner SDRs
- Assign nodes to the non-owner SDRs
- View the configured SDRs in the system.
- View and manage system-wide resources and logs.

See the "SDR Access Privileges" section on page SMC-130 for more information.

Note The Administration modes cannot be used to configure the features within a non-owner SDR, or view the router configuration for a non-owner SDR. After the SDR is created, users must log into the non-owner SDR directly to change the local configuration and manage the SDR. See the "Non-Owner SDRs" section on page SMC-130 for more information.

Non-Owner SDRs

To create a new non-owner SDR, the root-system user enters Administration configuration mode, defines a new SDR name, and assigns a set of cards to that SDR. Only a user with root-system privileges can access the commands in Administration configuration mode. Therefore, users without root-system privileges cannot create SDRs or assign cards to the SDRs.

After a non-owner SDR is created, the users configured on the non-owner SDR can log in and manage the router. The configuration for each non-owner SDR is separate from the owner SDR and can be accessed only by logging in to the non-owner SDR.

See the "SDR Access Privileges" section on page SMC-130 for more information.

Note For information regarding support for non-owner SDRs in the Cisco IOS XR software releases 2.0, 3.0, 3.2 and 3.3.0, see Software Version Requirements for the Cisco XR 12000 Series Router, page SMC-128.

SDR Access Privileges

Each SDR in a router has a separate AAA configuration that defines usernames, passwords, and associated privileges.

- Only users with root-system privileges can access the Administration EXEC and Administration configuration modes. See the "Root-System Users" section on page SMC-130 for more information.
- Users with root-lr privileges can access only the non-owner SDR in which that username was created. See the "root-lr Users" section on page SMC-131 for more information.
- Users with other access privileges can access features according to their assigned privileges for a specific SDR. See the "Other SDR Users" section on page SMC-131 for more information.

For more information about AAA policies, refer to *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Root-System Users

Users with root-system privileges have access to system-wide features and resources, including the ability to create and remove secure domain routers. The root-system user is created during the initial boot and configuration of the router.

The root-system user has the following privileges:

- Access to Administration EXEC and Administration configuration commands.
- Ability to create and delete non-owner SDRs.

- Ability to assign nodes (RPs, DRPs, and LCs) to SDRs.
- Ability to create other users with similar or lower privileges.
- Complete authority over the chassis.
- Ability to log in to non-owner SDRs using admin plane authentication. Admin plane authentication allows the root-system user to log in to a non-owner SDR regardless of the configuration set by the root-lr user. See the "Configuring a Username and Password for a Non-Owner SDR" section on page SMC-157
- Ability to install and activate software packages for all SDRs or for a specific SDR.
- Ability to view the following admin plane events (owner SDR logging system only):
  - Software installation operations and events.
  - System card boot operations, such as card booting notifications and errors, heartbeat-missed notifications, and card reloads.
  - Card alphanumeric display changes.
  - Environment monitoring events and alarms.
  - Fabric control events.
  - Upgrade progress information.

root-lr Users

Note SDRs were previously known as Logical Routers (LRs). The name was changed for Release 3.3.0.

Users with root-lr privileges can log in to the non-owner SDR only and perform configuration tasks that are specific to that SDR. The root-lr group has the following privileges:

- Ability to configure interfaces and protocols.
- Ability to create other users with similar or lower privileges on the non-owner SDR.
- Ability to view the resources assigned to their particular SDR.

The following restrictions apply to root-lr users:

- root-lr users cannot enter Administration EXEC or configuration modes.
- root-lr users cannot create or remove SDRs.
- root-lr users cannot add or remove nodes from an SDR.
- root-lr users cannot create root-system users.
- The highest privilege a non-owner SDR user can have is root-lr.

Other SDR Users

Additional usernames and passwords can be created by the root-system or root-lr users to provide more restricted access to the configuration and management capabilities of the owner SDR or non-owner SDRs.

Designated Secure Domain Router System Controller (DSDRSC)

In a router running the Cisco IOS XR software, one Route Processor is assigned the role of Designated System Controller (DSC). The DSC provides system-wide administration and control capability, including access to the Administration EXEC and Administration configuration modes. For more information on DSCs, refer to *Cisco IOS XR Getting Started Guide*.

In each SDR, similar administration and control capabilities are provided by the Designated Secure Domain Router System Controller (DSDRSC). Each SDR must include a DSDRSC to operate, and you must assign an RP or DRP to act as the dSDRSC.

Note In the owner SDR, the DSC also provides DSDRSC functionality.

The following sections describe DSDRSC support:

- DSCs and DSDRSCs in a Cisco CRS-1 Router, page SMC-132
- DSC and DSDRSCs in a Cisco XR 12000 Series Router, page SMC-133
- Removing a DSDRSC Configuration, page SMC-135

DSCs and DSDRSCs in a Cisco CRS-1 Router

Designated System Controller (DSC) in a Cisco CRS-1

In the Cisco CRS-1, the primary and standby DSC is always an RP pair. By default, the DSC is also the DSDRSC for the owner SDR. The owner DSDRSCs cannot be removed from the SDR configuration, or assigned to a non-owner SDR.

For information on DSC assignment and initial router configuration, refer to *Cisco IOS XR Getting Started Guide*.

Using a DRP or DRP Pair as the DSDRSC in a Cisco CRS-1 Router

Cisco Systems recommends the use of DRPs as the DSDRSC in non-owner SDRs to ensure DSC migration capability, as described in the "DSC Migration on Cisco CRS-1 Multishelf Systems" section on page SMC-136.

To create a DRP DSDRSC in a non-owner SDR, you must configure a DRP or DRP pair as the **primary** node for that SDR. The following guidelines apply:

- Although a single DRP can be used as the DSDRSC, we recommend the use of a redundant DRP pair.
- To create a DRP pair and configure it as the DSDRSC, complete the instructions in the "Creating SDRs in a Cisco CRS-1 Router" section on page SMC-140.
- DRPs cannot be used as the DSC in the owner SDR. Only RPs can be used as the DSC in the owner SDR.
- DRPs cannot be assigned as the DSDRSC if an RP is present in the SDR. To assign a DRP as the DSDRSC, you must first remove any RPs from the SDR configuration, and then add the DRP or DRP pair as the primary node. After the DRP is assigned as the DSDRSC, the RPs can be added to the SDR. See the "How to Configure Secure Domain Routers" section on page SMC-140 for more information.

- DRPs are supported in the Cisco CRS-1 only. DRPs are not supported in the Cisco XR 12000 Series Routers.

Note DRPs can also be used to provide additional processing capacity in a Cisco CRS-1 router. For additional information on DRPs, refer to *Cisco CRS-1 Carrier Routing System 16-Slot Line Card Chassis System Description*. For instructions on installing DRPs, refer to *Installing the Cisco CRS-1 Carrier Routing System 16-Slot Line Card Chassis*. For information on using DRPs for additional processing capacity, see the *Process Placement on Cisco IOS XR Software* module in the *Cisco IOS XR System Management Configuration Guide*.

Using a RP Pair as the DSDRSC in a Cisco CRS-1 Router

In a Cisco CRS-1 router, RP pairs can also be used as the DSDRSC in non-owner SDRs.

- Single RPs cannot be used as the DSDRSC.
- Redundant RPs in a CRS-1 Series router are installed in slots RP0 and RP1 of each line card chassis.
- To assign an RP pair as the DSDRSC, complete the instructions in the "How to Configure Secure Domain Routers" section on page SMC-140.

Note Although an RP pair can be used as the DSDRSC in non-owner SDRs, we recommend the use of a redundant DRP pair to ensure DRP migration capability. See the "DSC Migration on Cisco CRS-1 Multishelf Systems" section on page SMC-136 for more information.

DSC and DSDRSCs in a Cisco XR 12000 Series Router

In a Cisco XR 12000 Series Router, you can use a single RP or a redundant RP pair as the DSDRSC for each SDR. Redundant RP pairs must be installed in adjacent redundancy slots. The adjacent redundancy slots are as follows:

- Slot 0 and Slot 1
- Slot 2 and Slot 3
- Slot 4 and Slot 5
- Slot 6 and Slot 7
- Slot 8 and Slot 9
- Slot 10 and Slot 11
- Slot 12 and Slot 13
- Slot 14 and Slot 15

Review the additional information in this section for restrictions regarding RP usage in Cisco XR 12000 Series Routers.

Note Only two RPs can be operational in any SDR on a Cisco XR 12000 Series Router.

Note DRPs are not supported in Cisco XR 12000 Series Routers.

Designated System Controller (DSC) in a Cisco XR 12000 Series Router

- The first RP to be booted with the Cisco IOS XR software in a Cisco XR 12000 Series Router will become the Designated System Controller (DSC) for the router. This DSC is also the DSDRSC for the owner SDR. The DSC (owner DSDRSC) cannot be removed from the router configuration or reassigned to another SDR. For more information on bringing up a router for the first time, refer to *Cisco IOS XR Getting Started Guide*.
- A second RP can be used as the standby DSC. The standby DSC is also the standby DSDRSC for the owner SDR. The RP becomes the standby DSC if the following conditional are met:
  - The RP is installed in an adjacent redundancy slot to the DSC.
  - The RP is booted with the Cisco IOS XR software.
- Additional RPs can be installed in the router, but they will be non-operational until the following conditions are met:
  - The additional RPs are booted with the Cisco IOS XR software.
  - The RPs are added to a non-owner SDR configuration.

Designated Secure Domain Router System Controller (DSDRSC) in a Cisco XR 12000 Series Router

- Up to two RPs can be added to a non-owner SDR configuration.
- The first RP running the Cisco IOS XR software that is added to the SDR configuration will become the DSDRSC.
- If a second RP running the Cisco IOS XR software is installed in an adjacent redundancy slot, it will become the standby DSDRSC when added to the SDR configuration.
- If two RPs running the Cisco IOS XR software are installed in adjacent redundancy slots and are added to a new SDR at the same time, they will automatically elect a DSDRSC and standby DSDRSC between them.
- Any RPs added to the SDR that are not in the adjacent redundancy slot to the DSDRSC will be non-operational.

Note Additional RPs that are not the DSDRSC or standby DSDRSC can be added to an SDR configuration, but they will not be operational. These additional RPs will repetitively reset to prevent them from booting and interfering with other cards in the SDR. In addition, the DSC console will display repetitive error messages. We recommend that you either remove RP cards or assign them to a different SDR.

- Once a DSDRSC is configured for an SDR, an RP installed in the adjacent redundancy slot can only be assigned to that SDR. This is because adjacent redundancy slots form a redundancy pair that cannot be separated by SDR boundaries. For example, if the DSDRSC is installed in slot 2, an RP installed in slot 3 can only be assigned to the same SDR (as the standby DSDRSC).
- RPs that are installed on slots that are not adjacent redundancy slots can be assigned to different SDRs. For example, two RPs installed in slot 0 and slot 1 can only be configured as the DSDRSC and standby DSDRSC because they are installed in adjacent redundancy slots. However, two RPs installed in slot 1 and slot 2 can be used for different SDRs because these are not adjacent redundancy slots.

Removing a DSDRSC Configuration

There are two ways to remove a DSDRSC from an SDR:

- First remove all other nodes from the SDR configuration, and then remove the DSDRSC node. You cannot remove the DSDRSC node when other nodes are in the SDR configuration.
- Remove the entire SDR. Removing an SDR name deletes the SDR and moves all nodes back to the owner SDR inventory.

See the "Removing Nodes and SDRs" section on page SMC-151 for more information.

Default Configuration for New Non-Owner SDRs

Be default, the configuration of a new SDR is blank. The first configuration step after creating an SDR is to log in to the new non-owner SDR using admin plane authentication and create a username and password. You can then log out of the SDR and log back in using the new username and password. See the "Configuring a Username and Password for a Non-Owner SDR" section on page SMC-157 for more information.

Note When logged in to a non-owner SDR using admin plane authentication, the admin configuration will be displayed. However, admin plane authentication should only be used to configure a username and password for the non-owner SDR. To perform additional configuration tasks, log in with the username for the non-owner SDR, as described in the "Configuring a Username and Password for a Non-Owner SDR" section on page SMC-157.

Default Software Profile for SDRs

When a new non-owner SDR is created, the nodes assigned to that SDR are activated with the default software package profile. In Release 3.4.0, the default software profile is defined by the last install operation that did not specify an SDR.

To view the default software profile, use the **show install active summary** command in Administration EXEC mode. Any new nodes that are configured to become a part of an SDR will boot with the default software profile listed in the output of this command.

```
RP/0/0/CPU0:router(admin)# show install active summary

Default Profile:
  SDRs:
    Owner
    sdr1
  Active Packages:
    disk0:c12k-sbc-3.3.0
    disk0:c12k-diags-3.3.0
    disk0:c12k-mgbl-3.3.0
    disk0:c12k-mcast-3.3.0
    disk0:c12k-mpls-3.3.0
    disk0:c12k-k9sec-3.3.0
    disk0:c12k-mini-3.3.0
```

Note For detailed instructions to add and activate software packages, see the "Managing Cisco IOS XR Software Packages" module of the *Cisco IOS XR Getting Started Guide*. See also the *Software Package Management Commands on Cisco IOS XR Software* module of the *Cisco IOS XR System Management Command Reference*.

High Availability Implications

Fault Isolation

Because the CPU and memory of an SDR are not shared with other SDRs, configuration problems that cause out-of-resources conditions in one SDR do not affect other SDRs.

Rebooting an SDR

Each non-owner SDR can be rebooted independently of the other SDRs in the system. If you reboot the owner SDR, however, then all non-owner SDRs in the system automatically reboot, because the non-owner SDRs rely on the owner SDR for basic chassis management functionality.

Note The DSDRSC of the owner SDR is also the DSC of the entire system.

DSDRSC Redundancy

To achieve full redundancy, each SDR must be assigned two cards: one to act as the primary DSDRSC, and one RP or DRP to act as a standby DSDRSC.

In a Cisco XR 12000 Series Router, you can assign two redundant RP cards to each SDR as described in the "DSC and DSDRSCs in a Cisco XR 12000 Series Router" section on page SMC-133. DRPs are not supported in the Cisco XR 12000 Series Routers.

In a Cisco CRS-1 router, we recommend the use of DRP pairs as DSDRSC for all non-owner SDRs the system. DRP pairs provide redundancy within the SDR, and DSC migration for the entire system. See the following section for more information.

DSC Migration on Cisco CRS-1 Multishelf Systems

Designated Shelf Controller (DSC) migration is the act of moving the DSC role to a different part of the router. The DSC role automatically migrates when the DSC cannot perform its function on the shelf in which it currently resides. The cause of a DSC migration can be a failure of both of the RPs in the DSC shelf or any event that removes power from the DSC line card chassis (LCC).

DSC migration can be triggered by the following methods:

1. Shutdown power to DSC LCC. (Recommended)
2. Hardware-module reset or shutdown of a standby RP then an active RP in a DSC LCC. (Not recommended)
3. Online, insertion, removal (OIR) for an active RP and standby RP in a DSC LCC simultaneously. (Not recommended)
4. Removal of control Ethernet connectivity to both RPs in a DSC LCC. (Not recommended)

Note If planned downtime of a DSC LCC occurs, the recommended method of triggering DSC migration is to shutdown the power to the DSC LCC. The methods, which are not recommended, shutdown only one transport medium in the system. For example, control Ethernet but fabric medium can still be up for

another 30 seconds. This causes an inconsistent system view in the named SDR using DRP paired across the rack in which the DRP loses control Ethernet connectivity, but the LR plane is still working and can bring the named SDR into an inconsistent view if the named SDR is across the rack.

To support DSC migration in Cisco IOS XR Software Release 3.3.2 and higher, we recommend that you:

- Keep the default placement of all four RPs in the owner SDR. When the owner SDR spans both LCCs, the impact on the SDR resources is minimal in the remaining rack. Existing connections are not interrupted for the resources in the remaining rack, but a delay in routing new connections can occur while the routing tables are updated.
- Run all routing protocols in a named SDR. In addition, by running all routing protocols in a named SDR, which requires a distributed route processor (DRP) paired across the rack, the operation of Cisco Nonstop Forwarding (NSF) and Cisco Nonstop Routing (NSR) continues.

An election process selects the node that is to receive the DSC role upon DSC migration. The basis of the election is the shelf number. The shelf with the lowest number is designated to receive the DSC role.

DSC migration can cause a very short interruption to traffic flowing through the owner SDR. Although the time can vary with the addition of new features to DSC management and other factors, in the current release the time is likely to be around 20 to 30 seconds.

The reason for the traffic loss is because virtual Interfaces (VI), such as loopback, null, tunnels, and bundles are hosted on the DSDRSC of an SDR. For the owner SDR, the DSDRSC is the same node as the DSC itself. For DSC migration to occur, both active and standby DSC must be lost. Therefore, for the owner SDR, both active and standby DSDRSC are lost. VI's must be recreated on the new DSC, which is also the new DSDRSC. This operation takes some time, during which routing protocols such as BGP that use loopback or null interfaces are affected. Similarly, tunnels and bundles must also be recreated, affecting protocols such as MPLS. As a result, there is a drop in traffic in the default or owner SDR.

Note In Cisco IOS XR Software Release 3.3.0 and higher, DSC migration is disabled if the RPs in both LCCs are assigned to different SDRs.

To minimize the impact of DSC migration, create named SDRs that operate on DRP in each LCC. If the DSC rack fails, any named SDRs on the failed rack also fail. However, named SDRs on the unaffected rack can continue through DSC migration without any interruption in service. If the failure in the DSC rack affects only the RP cards, the named SDR in the affected rack cannot function after the RPs on that rack go down.

Cisco IOS XR Software Package Management

Software packages are added to the DSC of the system from Administration Exec mode. Once added, a package can be activated for all SDRs in the system, or for a specific SDR.

Note In Release 3.3.0, SDR-specific activation is supported for specific packages and upgrades, such as optional packages and SMUs. Packages that do not support SDR-specific activation can only be activated for all SDRs in the system. For detailed instructions, see the “Managing Cisco IOS XR Software Packages” module of the *Cisco IOS XR Getting Started Guide*. See also the “Software Package Management Commands on Cisco IOS XR Software” module of the *Cisco IOS XR System Management Command Reference*.

- To access **install** commands, you must be a member of the root-system user group with access to the Administration EXEC mode.
- Most **show install** commands can be used in the EXEC mode of an SDR to view the details of the active packages for that SDR.

Note For information, see Default Configuration for New Non-Owner SDRs, page SMC-135

DSC Migration on Cisco CRS-1 Multishelf Systems

Designated Shelf Controller (DSC) migration is the act of moving the DSC role to a different part of the router. The DSC role automatically migrates when the DSC cannot perform its function on the shelf in which it currently resides. The cause of a DSC migration can be a failure of both of the RPs in the DSC shelf or any event that removes power from the DSC line card chassis (LCC).

DSC migration can be triggered by the following methods:

1. Shutdown power to DSC LCC. (Recommended)
2. Hardware-module reset or shutdown of a standby RP then an active RP in a DSC LCC. (Not recommended)
3. Online, insertion, removal (OIR) for an active RP and standby RP in a DSC LCC simultaneously. (Not recommended)
4. Removal of control Ethernet connectivity to both RPs in a DSC LCC. (Not recommended)

Note If planned downtime of a DSC LCC occurs, the recommended method of triggering DSC migration is to shutdown the power to the DSC LCC. The methods, which are not recommended, shutdown only one transport medium in the system. For example, control Ethernet but fabric medium can still be up for another 30 seconds. This causes an inconsistent system view in the named SDR using DRP paired across the rack in which the DRP loses control Ethernet connectivity, but the LR plane is still working and can bring the named SDR into an inconsistent view if the named SDR is across the rack.

To support DSC migration in Cisco IOS XR Software Release 3.3.2 and higher, we recommend that you:

- Keep the default placement of all four RPs in the owner SDR. When the owner SDR spans both LCCs, the impact on the SDR resources is minimal in the remaining rack. Existing connections are not interrupted for the resources in the remaining rack, but a delay in routing new connections can occur while the routing tables are updated.
- Run all routing protocols in a named SDR. In addition, by running all routing protocols in a named SDR, which requires a distributed route processor (DRP) paired across the rack, the operation of Cisco Nonstop Forwarding (NSF) and Cisco Nonstop Routing (NSR) continues.

An election process selects the node that is to receive the DSC role upon DSC migration. The basis of the election is the shelf number. The shelf with the lowest number is designated to receive the DSC role.

DSC migration can cause a very short interruption to traffic flowing through the owner SDR. Although the time can vary with the addition of new features to DSC management and other factors, in the current release the time is likely to be around 20 to 30 seconds.

The reason for the traffic loss is because virtual Interfaces (VI), such as loopback, null, tunnels, and bundles are hosted on the DSDRSC of an SDR. For the owner SDR, the DSDRSC is the same node as the DSC itself. For DSC migration to occur, both active and standby DSC must be lost. Therefore, for the owner SDR, both active and standby DSDRSC are lost. VI's must be recreated on the new DSC,

which is also the new DSDRSC. This operation takes some time, during which routing protocols such as BGP that use loopback or null interfaces are affected. Similarly, tunnels and bundles must also be recreated, affecting protocols such as MPLS. As a result, there is a drop in traffic in the default or owner SDR.

Note In Cisco IOS XR Software Release 3.3.0 and higher, DSC migration is disabled if the RPs in both LCCs are assigned to different SDRs.

To minimize the impact of DSC migration, create named SDRs that operate on DRP in each LCC. If the DSC rack fails, any named SDRs on the failed rack also fail. However, named SDRs on the unaffected rack can continue through DSC migration without any interruption in service. If the failure in the DSC rack affects only the RP cards, the named SDR in the affected rack cannot function after the RPs on that rack go down.

Caveats

The following caveats apply to SDR creation and configuration:

- DRPs are supported for the DSDRSC in the Cisco CRS-1 only. DRPs are not supported in the Cisco XR 12000 Series Routers.
- In the Cisco CRS-1 router, we recommend the configuration of DRP pairs as the DSDRSC for all non-owner SDRs, as described in the "Using a DRP or DRP Pair as the DSDRSC in a Cisco CRS-1 Router" section on page SMC-132.
- Single RPs are not supported for the DSDRSC in Cisco CRS-1 routers. RPs must be installed and configured in redundant pairs.
- Single RPs and redundant RP pairs are supported for the DSDRSC on the Cisco XR 12000 Series Routers.
- LC admin plane events are displayed only on the non-owner SDR.
- Some admin plane debug events are not displayed on the owner SDR. For example, a non-owner card cannot send debug events to the DSC, which limits the debugging of Administration processes to the non-owner SDR.

How to Configure Secure Domain Routers

To create an SDR, configure an SDR name and then add nodes to the configuration. In Cisco CRS-1 routers, at least one node in each SDR must be explicitly configured as the DSDRSC. In the Cisco XR 12000 Series Router, the DSDRSC is created automatically when you add an RP to the configuration.

After the SDR is created, you can add or remove additional nodes and create a username and password for the SDR. See the following sections for instructions.

Contents

This section includes the following topics:

Creating SDRs

The following sections provide instructions to create new non-owner SDRs.

Creating SDRs in a Cisco CRS-1 Router

To create a non-owner SDR in a Cisco CRS-1 router, create an SDR name, add a DSDRSC, and then add additional nodes to the configuration. After the SDR is created, you can create a username and password for the SDR to allow additional configuration.

Note The Cisco CRS-1 supports a maximum of eight SDRs, including one owner SDR and up to seven non-owner SDRs.

Complete the following steps to create a non-owner SDR.

Note The procedures in this section can be performed only on a router that is already running the Cisco IOS XR software. For instructions to boot a router and perform the initial configuration, see the *Cisco IOS XR Getting Started Guide*. When a router is booted, the owner SDR is automatically created, and cannot be removed. This also includes instructions to create owner SDR username and password.

SUMMARY STEPS

1. **admin**
2. **configure**
3. (Optional) **pairing** *pair-name*
4. (Optional) **location** *partially-qualified-nodeid partially-qualified-nodeid*
5. (Optional) **exit**
6. **sdr** *sdr-name*
7. **pair** *pair-name* **primary**
   or
   location *partially-qualified-nodeid* **primary**
8. **location** *partially-qualified-nodeid*
   or
   pair *pair-name*
9. Repeat Step 8 as needed to add nodes to an SDR.
10. **exit**
11. Repeat Step 3 through Step 10 as needed to create additional secure domain routers.
12. **end**
    or
    commit
13. Create a username and password for the new SDR as described in the "Configuring a Username and Password for a Non-Owner SDR" section on page SMC-157.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters Administration EXEC mode.
Step 2	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Enters Administration configuration mode.
Step 3	**pairing** *pair-name* **Example:** `RP/0/RP0/CPU0:router(admin-config)# pairing drp1`	(Optional) Enter DRP pairing configuration mode. If the DRP name does not exist, the DRP pair is created when you add nodes, as described in the following step. • *pair-name* can be between 1 and 32 alphanumeric characters. The characters '_' or '-' are also allowed. All other characters are invalid. DRP pairs are used as the DSDRSC for a non-owner SDR, as described in the "DSCs and DSDRSCs in a Cisco CRS-1 Router" section on page SMC-132. **Note** Although a single DRP can be used as the DSDRSC in a non-owner SDR, Cisco systems recommends that two redundant DRPs be installed and assigned to the SDR. **Note** DRPs can also be added to an SDR to provide additional processing capacity. See the "Related Documents" section on page SMC-164 for more information on DRP installation and configuration.
Step 4	**location** *partially-qualified-nodeid* *partially-qualified-nodeid* **Example:** `RP/0/RP0/CPU0:router(admin-config-pairing:drp1)#` `location 0/3/* 0/4/*`	(Optional) Specifies the location of the DRPs in a DRP pair. The *partially-qualified-nodeid* argument is entered in the *rack/slot/** notation. Node IDs are always specified at the slot level, so the wildcard (*) is used to specify the CPU.
Step 5	**exit** **Example:** `RP/0/RP0/CPU0:router(admin-config-pairing:drp1)#` `exit`	(Optional) Exits the DRP pairing configuration mode and returns to Administration configuration mode. Complete this step only if you created a DRP pair.
Step 6	**sdr** *sdr-name* **Example:** `RP/0/RP0/CPU0:router(admin-config)# sdr rname2`	Enters the SDR configuration sub-mode for the specified SDR. • If this SDR does not yet exist, it is created when you add a node, as described in step 7. • If this SDR existed previously, you can add additional slots as described in step 7 and step 8.

	Command or Action	Purpose
Step 7	**pair** *pair-name* **primary** or **location** *partially-qualified-nodeid* **primary** **Example:** `RP/0/RP0/CPU0:router(admin-config-sdr:rname 2)# pair drp1 primary` `or` `RP/0/RP0/CPU0:router(admin-config-sdr:rname 2)# location 0/0/* primary` `or` `RP/0/RP0/CPU0:router(admin-config-sdr:rname 2)# location 0/RP*/* primary`	Specifies a DSDRSC for the non-owner SDR. You can assign a redundant DRP pair, an RP pair, or a single DRP as the DSDRSC. You cannot assign a single RP as the DSDRSC. Every SDR must contain a DSDRSC. • We recommend the use of DRP pairs as the DSDRSC for all non-owner SDRs to ensure DSC migration in a Cisco CRS-1 system. See the "DSC Migration on Cisco CRS-1 Multishelf Systems" section on page SMC-136 for more information. • The **primary** keyword configures the RPs, DRP pair, or DRP as the DSDRSC. If the **primary** keyword is not used, the node is assigned to the SDR, but it is not be the DSDRSC. • If an RP is already assigned to the SDR, it must be removed before a DRP or DRP pair can be assigned as the DSDRSC. See the "Removing Nodes from a Secure Domain Router in a Cisco CRS-1 Router" section on page SMC-152. **To assign a DRP pair as the DSDRSC** To assign a DRP pair as the DSDRSC, you must first create a DRP pair, as described in step 3 and step 4. After the DRP pair is created, you can add the pair to the configuration with the command **pair** *pair-name.* To assign the pair as the DSDRSC, use the **primary** keyword. **To assign a single DRP node as the DSDRSC** The value of the *partially-qualified-nodeid* argument is entered in the *rack/slot/** notation. The node ID is specified at the slot level, so the wildcard (*) is used to specify the CPU. **To assign an RP pair as the DSDRSC** The value of the *partially-qualified-nodeid* argument for RPs is entered in the *rack/RP*/** notation. This command assigns the redundant RP pair as the DSDRSC. One RP is automatically elected as the DSDRSC, and the second RP acts as the standby DSDRSC.

	Command or Action	Purpose
Step 8	**location** *partially-qualified-nodeid* or **location** *pair-name* **Example:** `RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# location 0/0/*` or `RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# location drp1` or `RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# location 0/RP*/*`	Adds additional nodes, DRP pairs, or RP pairs to the SDR. **To add a single node** Enter the **location** *partially-qualified-nodeid* command. The value of the *partially-qualified-nodeid* argument is entered in the *rack/slot/** notation. Node IDs are always specified at the slot level, so the wildcard (*) is used to specify the CPU. **To add a DRP pair** You must first create a pair, as described in step 3 and step 4. After the DRP pair is created, enter the **location** *pair-name* command. **To add an RP pair** Enter the **location** *partially-qualified-nodeid* command. The value of the *partially-qualified-nodeid* argument for RPs is entered in the *rack/RP*/** notation. This command assigns the redundant RP pair to the SDR. You cannot assign single RPs to an SDR in the Cisco CRS-1. **Note** See the "Adding Nodes to a Non-Owner SDR" section on page SMC-148 for more information.
Step 9	Repeat Step 8 as needed to add nodes to an SDR	Adds additional nodes to the SDR.
Step 10	**exit**	(Optional) Exits the SDR configuration submode and returns to Administration configuration mode. **Note** Complete this step only if you need to create additional SDRs.
Step 11	Repeat Step 3 through Step 10 as needed.	Creates additional SDRs.
Step 12	**end** or **commit** **Example:** `RP/0/RP0/CPU0:router (admin-config-sdr:rname2)# end` or `RP/0/RP0/CPU0:router(admin-config-sdr:rname)# commit`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found. Commit them?` – Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering **cancel** leaves the user in the same command mode without committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.
Step 13	Create a username and password for the new SDR.	(Optional) Refer to the "Configuring a Username and Password for a Non-Owner SDR" section on page SMC-157.

Creating SDRs in a 12000 Series Router

To create a non-owner SDR in a Cisco XR 12000 Series Router, create an SDR name, add an RP (that can act as DSDRSC) or 2 RPs in adjacent redundancy slots (that can act as the DSDRSC & standby DSDRSC) and then add additional (non-RP) nodes to the configuration

Note The procedures in this section can only be performed on a router that is already running the Cisco IOS XR software. For instructions to boot a router and perform the initial configuration, refer to *Cisco IOS XR Getting Started Guide*. When a router is booted, the owner SDR is automatically created, and cannot be removed. This guide also includes instructions to create owner SDR username and password.

Complete the following steps to create a non-owner SDR.

SUMMARY STEPS

1. **admin**
2. **configure**
3. **sdr** *sdr-name*
4. **location** *partially-qualified-nodeid*
5. (Optional) **location** *partially-qualified-nodeid*
6. **location** *partially-qualified-nodeid*
7. Repeat Step 6 as needed to add additional nodes to an SDR.
8. **exit**
9. Repeat Step 3 through Step 7 as needed to create additional SDRs.
10. **end**
    or
    commit
11. Create a username and password for the new SDR as described in the "Configuring a Username and Password for a Non-Owner SDR" section on page SMC-157.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/0/CPU0:router# admin`	Enters admin mode.
Step 2	**configure** **Example:** `RP/0/0/CPU0:router(admin)# configure`	Enters Administration configuration mode.

	Command or Action	Purpose
Step 3	**sdr** *sdr-name* **Example:** `RP/0/0/CPU0:router(admin-config)# sdr rname`	Enters the Administration configuration mode for the specified SDR. • If this SDR does not yet exist, it is created when you add a node as described in the following step. • If this SDR existed previously, complete the following steps to add additional nodes. **Note** For the Cisco XR 12000 Series Router, we recommend a maximum of four SDRs, including one owner SDR and up to three non-owner SDRs.
Step 4	**location** *partially-qualified-nodeid* **Example:** `RP/0/0/CPU0:router(admin-config-sdr:rname)# location 0/0/*`	Assigns an RP node as the DSDRSC for the non-owner SDR. On a Cisco XR 12000 Series Router, you can assign a single RP or a redundant RP pair as the DSDRSC. • The first RP you assign to the SDR becomes the DSDRSC. • To add a redundant standby RP to the configuration, a second RP must be installed in the adjacent redundancy slot and added to the SDR configuration. See the "DSC and DSDRSCs in a Cisco XR 12000 Series Router" section on page SMC-133 for information on redundancy slots. See Step 5 for instructions to add an additional RP to the configuration. • The value of the *partially-qualified-nodeid* argument is entered in the *rack/slot/** notation. The node ID is specified at the slot level, so the wildcard (*) is used to specify the CPU. • DRPs are not supported in Cisco XR 12000 Series Routers.
Step 5	**location** *partially-qualified-nodeid* **Example:** `RP/0/0/CPU0:router(admin-config-sdr:rname)# location 0/1/*`	(Optional) Assigns a second RP to act as the standby DSDRSC. If an RP is in an adjacent redundancy slot to the DSDRSC, then the RP automatically becomes the standby DSDRSC. • See the "DSC and DSDRSCs in a Cisco XR 12000 Series Router" section on page SMC-133 for more information. • The value of the *partially-qualified-nodeid* argument is entered in the *rack/slot/** notation. The node ID is specified at the slot level, so the wildcard (*) is used to specify the CPU. • Although single RPs are supported in Cisco XR 12000 Series Routers, we recommend the use of a redundant RP pair: one to act as the DSDRSC and the second to act as a standby DSDRSC.

	Command or Action	Purpose
Step 6	**location** *partially-qualified-nodeid* **Example:** `RP/0/0/CPU0:router(admin-config-sdr:rname)# location 0/5/*`	Assigns additional nodes to the SDR. • Enter the value of the *partially-qualified-nodeid* argument to specify a single node. The value of the *nodeid* argument is entered in the *rack/slot/** notation. Node IDs are always specified at the slot level, so the wildcard (*) is used to specify the CPU. • Refer to the "Adding Nodes to a Non-Owner SDR" section on page SMC-148 for more information.
Step 7	Repeat Step 6 as needed to add additional nodes to the SDR.	Adds additional nodes to the SDR.
Step 8	**exit**	(Optional) Exits the SDR configuration submode and returns to Administration configuration mode. **Note** Complete this step only if you need to create additional SDRs.
Step 9	Repeat Step 3 through Step 7 as needed to create additional SDRs.	Creates additional SDRs.
Step 10	**end** or **commit** **Example:** `RP/0/0/CPU0:router (admin-config-sdr:rname)# end` or `RP/0/0/CPU0:router(admin-config-sdr:rname)# commit`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found. Commit them?` – Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering **cancel** leaves the user in the same command mode without committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.
Step 11	Create a username and password for the new SDR.	(Optional) Refer to the "Configuring a Username and Password for a Non-Owner SDR" section on page SMC-157.

Adding Nodes to a Non-Owner SDR

When adding nodes to an existing non-owner SDR, the following rules apply:

- By default, all nodes in a new system belong to the owner SDR. When a node is assigned to a non-owner SDR, the node is removed from the owner SDR inventory and added to the non-owner SDR.
- When a node is removed from a non-owner SDR, it is automatically returned to the owner SDR inventory.
- To add a node that already belongs to another non-owner SDR, you must first remove the node from the other SDR, and then reassign it to the new SDR. See the "Removing Nodes from a Secure Domain Router in a Cisco CRS-1 Router" section on page SMC-152 for more information.
- You cannot assign the DSC or standby DSC to a non-owner SDR. The DSC and standby DSC can cannot be removed and assigned to a non-owner SDR.
- The main difference between adding a node in a Cisco CRS-1 and a Cisco XR 12000 Series Router is for DSDRSC support:
  - Cisco CRS-1 routers support DRPs and DRP pairs.
  - In a Cisco CRS-1 router, RPs can only be added in redundant pairs.
  - Cisco XR 12000 Series Routers do not support DRPs.
  - In a Cisco XR 12000 Series Router, RPs can be added individually or in redundant sets. Only two RPs (if installed in the adjacent redundancy slots) can function in each SDR.

Complete the following steps to add one or more nodes to an existing non-owner SDR:

- Adding Nodes to an SDR in a Cisco CRS-1 Router, page SMC-148
- Adding Nodes to an SDR in a Cisco XR 12000 Series Router, page SMC-150

Adding Nodes to an SDR in a Cisco CRS-1 Router

SUMMARY STEPS

1. **admin**
2. **configure**
3. **sdr** *sdr-name*
4. **location** *partially-qualified-nodeid*
   or
   location *pair-name*
5. **end**
   or
   commit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters Administration EXEC mode.
Step 2	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Enters Administration configuration mode.
Step 3	**sdr** *sdr-name* **Example:** `RP/0/RP0/CPU0:router(admin-config)# sdr rname`	Enters the SDR configuration submode for the specified SDR. • *sdr-name* is the name assigned to the SDR.
Step 4	**location** *partially-qualified-nodeid* or **location** *pair-name* **Example:** `RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# location 0/0/*` or `RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# location drp1` or `RP/0/RP0/CPU0:router(admin-config-sdr:rname)# location 0/RP*/*`	Adds additional nodes, DRP pairs, or RP pairs to an SDR. **To add a single node** Enter the **location** *partially-qualified-nodeid* command. The value of the *partially-qualified-nodeid* argument is entered in the *rack/slot/** notation. Node IDs are always specified at the slot level, so the wildcard (*) is used to specify the CPU. **To add a DRP pair** You must you must first create a pair as described in step 3 and step 4 of Creating SDRs in a Cisco CRS-1 Router, page SMC-140. Once the DRP pair is created, enter the **location** *pair-name* command. *pair-name* is the name assigned to the DRP pair. **To add an RP pair** Enter the **location** *partially-qualified-nodeid* command. The value of the *partially-qualified-nodeid* argument for RPs is entered in the *rack/RP*/** notation. This command assigns the redundant RP pair to the SDR. You cannot assign single RPs to an SDR in the Cisco CRS-1.

	Command or Action	Purpose
Step 5	**end** or **commit** **Example:** `RP/0/RP0/CPU0:router (admin-config-sdr:rname2)# end` or `RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# commit`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found. Commit them?` – Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering **cancel** leaves the user in the same command mode without committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Adding Nodes to an SDR in a Cisco XR 12000 Series Router

SUMMARY STEPS

1. **admin**
2. **configure**
3. **sdr** *sdr-name*
4. **location** *partially-qualified-nodeid*
5. **end**
   or
   commit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/0/CPU0:router# admin`	Enters Administration EXEC mode.
Step 2	**configure** **Example:** `RP/0/0/CPU0:router(admin)# configure`	Enters Administration configuration mode.
Step 3	**sdr** *sdr-name* **Example:** `RP/0/0/CPU0:router(admin-config)# sdr rname`	Enters the SDR configuration submode for the specified SDR. • *sdr-name* is the name assigned to the SDR.

	Command or Action	Purpose
Step 4	**location** *partially-qualified-nodeid* **Example:** `RP/0/0/CPU0:router(admin-config-sdr:rname)# location 0/5/*`	Adds additional nodes to the SDR. • Enter the value of the *partially-qualified-nodeid* argument to specify a single node. The value of the *nodeid* argument is entered in the *rack/slot/** notation. Node IDs are always specified at the slot level, so the wildcard (*) is used to specify the CPU. • If you add an RP installed in a redundancy slot next to the DSDRSC, then the second RP becomes the standby DSDRSC. Refer to the "DSC and DSDRSCs in a Cisco XR 12000 Series Router" section on page SMC-133 for more information.
Step 5	**end** or **commit** **Example:** `RP/0/0/CPU0:router (admin-config-sdr:rname2)# end` or `RP/0/0/CPU0:router(admin-config-sdr:rname2)# commit`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found. Commit them?` – Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering **cancel** leaves the user in the same command mode without committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Removing Nodes and SDRs

This section contains the following instructions:

- Removing Nodes from a Secure Domain Router in a Cisco CRS-1 Router, page SMC-152
- Removing Nodes from a Secure Domain Router: Cisco XR 12000 Series Router, page SMC-154
- Removing a Secure Domain Router, page SMC-156

When removing a node or an entire SDR, the following rules apply:

- When a node is removed from a non-owner SDR, it is automatically returned to the owner SDR inventory.
- To remove a DSDRSC, first remove the other nodes in the SDR, and then remove the DSDRSC. This rule does not apply when the entire SDR is removed.
- If all nodes are removed from a non-owner SDR, the SDR name is also removed.
- To remove all nodes, including the DSDRSC, remove the SDR name. All nodes are returned to the owner SDR inventory.

- You must first remove a node from a non-owner SDR before it can be reassigned to another non-owner SDR.
- To remove a node from the owner SDR inventory, assign the node to an non-owner SDR.
- The owner SDR cannot be removed, and the owner DSDRSC (DSC) cannot be removed.

Removing Nodes from a Secure Domain Router in a Cisco CRS-1 Router

SUMMARY STEPS

1. **admin**
2. **configure**
3. **sdr** *sdr-name*
4. **no location** *partially-qualified-nodeid*
   or
   no location *pair-name*
5. **end**
   or
   commit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters Administration EXEC mode.
Step 2	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Enters Administration configuration mode.
Step 3	**sdr** *sdr-name* **Example:** `RP/0/RP0/CPU0:router(admin-config)# sdr rname`	Enters the SDR configuration submode for the specified SDR.

	Command or Action	Purpose
Step 4	**no location** *partially-qualified-nodeid* or **no location** *pair-name* **Example:** `RP/0/RP0/CPU0:router(admin-config-sdr:rname2)#` `no location 0/0/*` or `RP/0/RP0/CPU0:router(admin-config-sdr:rname2)#` `no location drp1` or `RP/0/RP0/CPU0:router(admin-config-sdr:rname)#` `no location 0/RP*/*`	Removes a node, DRP pair, or RP pair from a non-owner SDR. • When a node is removed from an SDR, it is automatically added to the owner SDR inventory. This node may now be assigned to a different SDR, as described in Adding Nodes to an SDR in a Cisco CRS-1 Router, page SMC-148. • Removing all the slots from an SDR deletes that SDR. **To remove a DSDRSC** The DSDRSC cannot be removed if other nodes are in the SDR configuration. To remove the DSDRSC, you must first remove all other nodes in the SDR. **To remove a single node** Enter the **no location** *partially-qualified-nodeid* command. The value of the *partially-qualified-nodeid* argument is entered in the *rack/slot/** notation. Node IDs are always specified at the slot level, so the wildcard (*) is used to specify the CPU. **To remove a DRP pair** Enter the **no location** *pair-name* command. The *pair-name* argument is the name assigned to the DRP pair. **To remove an RP pair** Enter the **no location** *partially-qualified-nodeid* command. The value of the *partially-qualified-nodeid* argument for RPs is entered in the *rack/RP*/** notation. This command removes both RPs in a pair.
Step 5	**end** or **commit** **Example:** `RP/0/RP0/CPU0:router (admin-config-sdr:rname2)# end` or `RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# commit`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found. Commit them?` – Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering **cancel** leaves the user in the same command mode without committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Removing Nodes from a Secure Domain Router: Cisco XR 12000 Series Router

SUMMARY STEPS

1. **admin**
2. **configure**
3. **sdr** *sdr-name*
4. **no location** *partially-qualified-nodeid*
5. **end**
   or
   commit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/0/CPU0:router# admin`	Enters Administration EXEC mode.
Step 2	**configure** **Example:** `RP/0/0/CPU0:router(admin)# configure`	Enters Administration configuration mode.
Step 3	**sdr** *sdr-name* **Example:** `RP/0/0/CPU0:router(admin-config)# sdr rname`	Enters the SDR configuration submode for the specified SDR.

	Command or Action	Purpose
Step 4	**no location** *partially-qualified-nodeid* **Example:** `RP/0/0/CPU0:router(admin-config-sdr:rname2)#` `no location 0/0/*`	Removes a node from a non-owner SDR. • When a node is removed from an SDR, it is automatically added to the owner SDR inventory. This node may now be assigned to a different SDR, as described in the "Adding Nodes to an SDR in a Cisco XR 12000 Series Router" section on page SMC-150. • Removing all the slots from an SDR deletes that SDR. **To remove a DSDRSC** The DSDRSC cannot be removed if other nodes are in the SDR configuration. To remove the DSDRSC, you must first remove all other nodes in the SDR. **To remove a single node** Enter the **no location** *partially-qualified-nodeid* command. The value of the *partially-qualified-nodeid* argument is entered in the *rack/slot/** notation. Node IDs are always specified at the slot level, so the wildcard (*) is used to specify the CPU.
Step 5	**end** or **commit** **Example:** `RP/0/RP0/CPU0:router (admin-config-sdr:rname2)# end` or `RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# commit`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found. Commit them?` – Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering **cancel** leaves the user in the same command mode without committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Removing a Secure Domain Router

This section provides instructions to remove a secure domain router from either a Cisco CRS-1 or a Cisco XR 12000 Series Router. To remove an SDR, you can either remove all the nodes in the SDR individually or remove the SDR name. This section contains instructions to remove the SDR name and return all nodes to the owner SDR inventory.

Note The owner SDR cannot be removed. Only non-owner SDRs can be removed.

SUMMARY STEPS

1. **admin**
2. **configure**
3. **no sdr** *sdr-name*
4. **end**
   or
   commit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters Administration EXEC mode.
Step 2	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Enters Administration configuration mode.
Step 3	**no sdr** *sdr-name* **Example:** `RP/0/RP0/CPU0:router(admin-config)# no sdr rname`	Removes the specified SDR from the current owner SDR. **Note** All slots belonging to that SDR return to the owner SDR inventory.

	Command or Action	Purpose
Step 4	**end** or **commit** **Example:** `RP/0/RP0/CPU0:router (admin-config)# end` or `RP/0/RP0/CPU0:router(admin-config)# commit`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found. Commit them?` – Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering **cancel** leaves the user in the same command mode without committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring a Username and Password for a Non-Owner SDR

After you create an SDR, you can create a username and password on that SDR. When you assign root-lr privileges to that username, the user can administer the non-owner SDR and create additional users if necessary.

Note Only users with root-system privileges can access Administration modes to add or remove SDRs. SDR users cannot add or remove SDRs.

To create a username and password for the new non-owner SDR.

1. On the owner SDR, enable admin plane authentication. This allows you to log in to the non-owner SDR and create local usernames and passwords.
2. Log in to the non-owner SDR.
3. Configure a new username and password on the non-owner SDR. Assign the username to the root-lr group to allow the creation of additional usernames on that SDR.
4. To verify the new username, log out and log back in to the non-owner SDR using the new username and password.
5. Provide the username and password to the SDR user.

Complete the following steps to create usernames and passwords on a non-owner SDR.

SUMMARY STEPS

1. Connect a terminal to the console port of the DSC (DSDRSC of the owner SDR).
2. **admin**
3. **configure**
4. **aaa authentication login remote local**

5. **end**
   or
   commit
6. Connect a terminal to the console port of the non-owner SDR DSDRSC.
7. Log in to the non-owner SDR using admin plane authentication:
   `Username:`*`username`***`@admin`**
   `Password:`*`xxxx`*
8. **configure**
9. **username** *username*
10. **secret** *password*
11. **group root-lr**
12. **end**
    or
    commit
13. **exit**
14. Username:*username*
    Password:*xxxx*
15. Provide the new username and password to the user.
16. Disable admin plane authentication as described in the "Disabling Remote Login for SDRs" section on page SMC-161.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Connect a terminal to the console port of the DSC (DSDRSC of the owner SDR).	**Note** If an IP address has not yet been assigned to the Management Ethernet port, you must connect a terminal directly to the console port of the DSC.
Step 2	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters Administration EXEC mode.
Step 3	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Enters Administration configuration mode.

	Command or Action	Purpose
Step 4	**aaa authentication login remote local** **Example:** `RP/0/RP0/CPU0:router(admin-config)# aaa authentication login remote local`	Enables admin plane authentication. • The **remote** keyword specifies a method list that uses remote non-owner SDR for authentication. • The **local** keyword specifies a method list that uses the local username database method for authentication. The local authentication cannot fail because the system always ensures that at least one user is present in the local database, and a rollover cannot happen beyond the local method. **Note** You can also use other methods to enable AAA system accounting, such as TACACS+ or RADIUS servers. See "Configuring AAA Services on Cisco IOS XR Software" module of the *Cisco IOS XR System Security Configuration Guide* for more information. **Note** When logged in to a non-owner SDR using admin plane authentication, the admin configuration will be displayed. However, admin plane authentication should only be used to configure a username and password for the non-owner SDR. To perform additional configuration tasks, log in with the username for the non-owner SDR, as described in the following steps.
Step 5	**end** or **commit** **Example:** `RP/0/RP0/CPU0:router (admin-config)# end` or `RP/0/RP0/CPU0:router(admin-config)# commit`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found. Commit them?` – Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering **cancel** leaves the user in the same command mode without committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.
Step 6	Connect a terminal to the console port of the non-owner SDR DSDRSC.	**Note** A terminal server connection is required for Telnet connections to the console port because an IP address has not yet been assigned to the management Ethernet port.

	Command or Action	Purpose
Step 7	Log in to the non-owner SDR using admin plane authentication: `Username:`*xxxx*`@admin` `Password:`*xxxx* **Example:** `Username:`*xxxx@admin* `Password:`*xxxx*	Logs a root-system user into the SDR using admin plane authentication. **Note** Where it says "Username:*xxxx*@**admin**," replace *xxxx* with your username.
Step 8	**configure** **Example:** `RP/0/RP0/CPU0:router# configure`	Enters configuration mode.
Step 9	**username** *username* **Example:** `RP/0/RP0/CPU0:router(config)# username user1`	Defines an SDR username and enters username configuration mode. The *user-name* argument can be only one word. Spaces and quotation marks are not allowed.
Step 10	**secret** *password* **Example:** `RP/0/RP0/CPU0:router(config-un)# secret 5 XXXX`	Defines a password for the user.
Step 11	**group root-lr** **Example:** `RP/0/RP0/CPU0:router(config-un)# group root-lr`	Adds the user to the predefined root-lr group. **Note** Only users with root-system authority or root-lr authority may use this option.
Step 12	**end** or **commit** **Example:** `RP/0/RP0/CPU0:router (config)# end` or `RP/0/RP0/CPU0:router(config)# commit`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found. Commit them?` – Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering **cancel** leaves the user in the same command mode without committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.
Step 13	**exit** **Example:** `exit`	Closes the active terminal session and log off the router.

	Command or Action	Purpose
Step 14	**Username:** *xxxx* **Password:** *xxxx* **Example:** `Press RETURN to get started.` `Username:user1` `Password:xxxxx`	Logs back in with the SDR administrator username and password you created. This username is used to configure the secure domain router and create other users with fewer privileges. • This step verifies proper SDR administrator username and password configuration. • After you create the SDR username and password, you need to provide the SDR username and password to the operators who will use that SDR.
Step 15	Provide the new username and password to the user.	
Step 16	Disable admin plane authentication.	See Disabling Remote Login for SDRs, page SMC-161 for more information.

Disabling Remote Login for SDRs

When you disable admin plane authentication, the admin username cannot be used to log in to non-owner SDRs. Only local SDR usernames can be used to log into the SDR.

SUMMARY STEPS

1. **admin**
2. **configure**
3. **no aaa authentication login remote local**
4. **end**
   or
   commit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters Administration EXEC mode.
Step 2	**configure** **Example:** `RP/0/RP0/CPU0:router(admin)# configure`	Enters Administration configuration mode.

	Command or Action	Purpose
Step 3	**no aaa authentication login remote local** **Example:** `RP/0/RP0/CPU0:router(admin-config)# no aaa authentication login remote local`	Disables remote login.
Step 4	**end** or **commit** **Example:** `RP/0/RP0/CPU0:router (admin-config)# end` or `RP/0/RP0/CPU0:router(admin-config)# commit`	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found. Commit them?` – Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering **cancel** leaves the user in the same command mode without committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuration Examples for Secure Domain Routers

Creating a New SDR on a Cisco CRS-1 Router

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# configure
RP/0/RP0/CPU0:router(admin-config)# pairing drp1
RP/0/RP0/CPU0:router(admin-config-pairing:drp1)# location 0/3/* 0/4/*
RP/0/RP0/CPU0:router(admin-config-pairing:drp1)#exit
RP/0/RP0/CPU0:router(admin-config)# sdr rname2
RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# pair pair1 primary
RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# location 0/0/*
RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# end
```

Creating an SDR on a Cisco XR 12000 Series Router

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# configure
RP/0/0/CPU0:router(admin-config)# sdr rname
RP/0/0/CPU0:router(admin-config-sdr:rname)# location 0/0/*
RP/0/0/CPU0:router(admin-config-sdr:rname)# location 0/1/*
RP/0/0/CPU0:router(admin-config-sdr:rname)# location 0/5/*
RP/0/0/CPU0:router(admin-config-sdr:rname)# end
```

Adding nodes to an SDR: Cisco CRS-1 Router

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# configure
RP/0/RP0/CPU0:router(admin-config)# sdr rname2
RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# location 0/0/*
RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# end
```

Adding nodes to an SDR: Cisco XR 12000 Series Router

```
RP/0/0/CPU0:router# admin
RP/0/0/CPU0:router(admin)# configure
RP/0/0/CPU0:router(admin-config)# sdr rname2
RP/0/0/CPU0:router(admin-config-sdr:rname2)# location 0/5/*
RP/0/0/CPU0:router (admin-config-sdr:rname2)# end
```

Removing Nodes from a Secure Domain Router: Cisco CRS-1 Router

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# configure
RP/0/RP0/CPU0:router(admin-config)# sdr rname2
RP/0/RP0/CPU0:router(admin-config-sdr:rname2)# no location 0/0/*
RP/0/RP0/CPU0:router (admin-config-sdr:rname2)# end
```

Removing a Secure Domain Router: Cisco CRS-1 Router

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# configure
RP/0/RP0/CPU0:router(admin-config)# no sdr rname2
RP/0/RP0/CPU0:router (admin-config)# end
```

Configuring a Username and Password for a Non-Owner SDR

Connect to the DSC of the owner SDR.

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# configure
RP/0/RP0/CPU0:router(admin-config)# aaa authentication login remote local
RP/0/RP0/CPU0:router (admin-config)# end
```

To continue, connect a terminal to the console port of the non-owner SDR DSDRSC.

```
Username:xxxx@admin
Password:xxxx
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# username user1
RP/0/RP0/CPU0:router(config-un)# secret 5 XXXX
RP/0/RP0/CPU0:router(config-un)# group root-lr
RP/0/RP0/CPU0:router (config)# end
RP/0/RP0/CPU0:router# exit

Press RETURN to get started.
Username:user1
Password:xxxxx
```

Disabling Remote Login for SDRs

```
RP/0/RP0/CPU0:router# admin
RP/0/RP0/CPU0:router(admin)# configure
RP/0/RP0/CPU0:router(admin-config)# no aaa authentication login remote local
RP/0/RP0/CPU0:router (admin-config)# end
```

Additional References

The following sections provide references related to SDR configuration.

Related Documents

Related Topic	Document Title
SDR command reference.	*Secure Domain Router Commands on Cisco IOS XR Software*
DRP pairing command reference.	*Distributed Route Processor Commands on Cisco IOS XR Software*
Initial system bootup and configuration information for a router using the Cisco IOS XR software.	*Cisco IOS XR Getting Started Guide*
DRP description and requirements.	*Cisco CRS-1 Carrier Routing System 16-Slot Line Card Chassis System Description*
Instructions to install DRP and DRP PLIM cards.	*Installing the Cisco CRS-1 Carrier Routing System 16-Slot Line Card Chassis*
Cisco IOS XR master command reference	*Cisco IOS XR Master Commands List*
Information about user groups and task IDs	*Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*
Cisco IOS XR interface configuration commands	*Cisco CRS-1 Series Interface and Hardware Component Command Reference*
Information about configuring interfaces and other components on the Cisco CRS-1 from a remote Craft Works Interface (CWI) client management application	*Cisco CRS-1 Series Carrier Routing System Craft Works Interface Configuration Guide*
Information about AAA policies, including instructions to create and modify users and username access privileges.	*Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport